This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A method of sending ~~encrypted~~ streamed data over an IP network from a first node to a second node, the method comprising:

using a first protocol to establish a first security association (SA1) ~~Internet Key Exchange (IKE) Phase 1 negotiation to establish an IKE security association (SA)~~ between the first and second nodes;

using the first protocol to establish a first security association (SA1) over a second protocol between the first and second nodes;

modifying the second security association (SA2) by using selected components of the second protocol for providing encryption at the first node of the streamed data between the first and second nodes;

constructing datagrams containing segments of the encrypted streamed data in the datagram payload, the datagrams including a reduced overhead corresponding to the selected components; and

sending the datagrams from the first node to the second node.

~~entering IKE Phase 2 to negotiate an IPSec SA for each transmission direction;~~

~~passing the IPSec SA data to streamed data applications associated with the streamed data;~~

~~encrypting the streamed data at the first node with a cipher using a shared secret forming part of said IPSec SA;~~

~~constructing IP datagrams containing the encrypted streamed data, the datagrams not including an IPSec header or headers; and~~

~~sending the IP datagrams from the first node to the second node.~~

2. (Currently Amended) A method according to claim 1, wherein said streamed data is VoIP data or videoconferencing data, wherein said streamed data

packets do not include IPSec headers, authentication headers (AH) and encapsulation security payload (ESP) headers.

3. (Previously Presented) A method according to claim 1, wherein said first and second nodes are end points for the data.

4. (Previously Presented) A method according to claim 1, wherein said first and second nodes tunnel data between respective end points.

5. (Currently Amended) An apparatus for sending ~~securing~~ streamed data over an IP network from a first node to a second node, the apparatus comprising:

processing means and memory containing software instructions for implementing IPSec protocols:

~~an application for delivering streamed data;~~

means for using a first protocol to establish a first security association (SA1) ~~Internet Key Exchange (IKE) Phase 1 negotiation to establish an IKE security association (SA)~~ between the first and second nodes;

means for using the first protocol to establish a first security association (SA1) over a second protocol between the first and second nodes;

means for modifying the second security association (SA2) by using selected components of the second protocol for providing encryption at the forst node of the streamed data between the first and second nodes;

means for constructing datagrams containing segments of the encrypted streamed data in the datagram payload, the datagrams including a reduced overhead corresponding to the selected components; and

means for sending the datagrams from the first node to the second node.

~~means for entering IKE Phase 2 negotiation to negotiate an IPSec SA for each transmission direction;~~

~~means for passing the IPSec SA data to applications associated with the streamed data;~~

~~encrypting means for encrypting the streamed data at the first node with a cipher using a shared secret forming part of said IPSec SA;~~

~~means for constructing IP datagrams containing the encrypted streamed data, the datagrams not including an IPSec header or headers; and~~

~~transmission means for sending the IP datagrams from the first node to the second node.~~

6. (Original) Apparatus according to claim 5, the apparatus being an end user terminal such as a telephone, communicator, PDA or palmtop computer, or a personal computer (PC).

7. (Currently Amended) Apparatus according to claim 6, the apparatus being a firewall or gateway coupled to the first node, which is the source of the streamed data, wherein the streamed data packets do not include IPSec headers, authentication headers (AH) and encapsulation security payload (ESP) headers.